UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,260	10/17/2001	Johan Paul Marie Gerard Linnartz	NL000558	7206

24737 7590 01/10/2008

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
BROWN, CHRISTOPHER J	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
01/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JOHAN PAUL MARIE GERARD LINNARTZ

Appeal 2007-1774
Application 09/982,260
Technology Center 2100

Decided: January 10, 2008

Before KENNETH W. HAIRSTON, ALLEN R. MACDONALD, and ST. JOHN COURTENAY III, *Administrative Patent Judges*.

HAIRSTON, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant appeals under 35 U.S.C. § 134 from a final rejection of claims 1 to 20. After submission of the brief, the Examiner allowed claims 6 and 7. Accordingly, claims 1 to 5 and 8 to 20 are before us on appeal. We have jurisdiction under 35 U.S.C. § 6(b).

We will sustain the rejection.

STATEMENT OF THE CASE

Appellant has invented a method for secure data communication for transferring content between consumer devices that comprises the steps of activating a communications link between the devices, performing an authentication session for authenticating the consumer devices by transmitting data between the devices to thereby create a first key, and performing a subsequent authentication session for authenticating the consumer devices by transmitting data between the devices to thereby create a second key. The second key is then used in transferring audio and visual content (Figures 1 and 2; Specification 2, 4, and 8).

Claim 1 is representative of the claims on appeal, and it reads as follows:

1. Method for secure data communication to transfer content between consumer devices, the method comprising the following steps: a) activating a data communication link between the devices, b) transmitting data between the devices for performing an authentication session for authenticating the consumer devices, wherein the authentication session generates a first key, characterized in that the method further comprises the step of:
c) transmitting data between the devices for performing a subsequent authentication session for authenticating the consumer devices, wherein the subsequent authentication session generates a second key used in transferring audio or visual content.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Holloway	US 5,604,802	Feb. 18, 1997
Herlin	US 5,915,021	Jun. 22, 1999
Jaisimha	US 6,487,663 B1	Nov. 26, 2002 (filed Oct. 19, 1998)
Moskowitz	US 6,598,162 B1	Jul. 22, 2003 (filed Mar. 24, 1998)
Crane	US 6,839,437 B1	Jan. 4, 2005 (filed Jan. 31, 2000)

Bluetooth Security, Bluetooth Specification Version 1.0 B, 149 to 178, (November 29, 1999).

The Examiner rejected claims 1, 3, 4, 9, 11 to 15, 17, and 19 under 35 U.S.C. § 103(a) based upon the teachings of Herlin and Jaisimha.

The Examiner rejected claims 2, 5, and 16 under 35 U.S.C. § 103(a) based upon the teachings of Herlin, Jaisimha, and the Bluetooth Security publication.

The Examiner rejected claim 8 under 35 U.S.C. § 103(a) based upon the teachings of Herlin, Jaisimha, and Holloway.

The Examiner rejected claim 10 under 35 U.S.C. § 103(a) based upon the teachings of Herlin, Jaisimha, and Crane.

The Examiner rejected claims 18 and 20 under 35 U.S.C. § 103(a) based upon the teachings of Herlin, Jaisimha, and Moskowitz.

Appellant contends *inter alia* that "[t]here is no disclosure or suggestion within *Herlin et al.* for a subsequent authentication, wherein the subsequent authentication session generates a second key" (Br. 7).

ISSUE

Does the applied prior art teach or would the applied prior art have suggested to the skilled artisan the steps of claim 1 including the generation of a second key during an authentication session between consumer devices?

FINDINGS OF FACT

As indicated *supra*, Appellant generates two keys during two different authentication sessions between consumer devices for secure transfer of data content between the consumer devices.

Herlin describes a method for secure data communication between consumer devices (e.g., cellular telephones) (Figure 2; Title; Abstract; col. 1, ll. 11 to 27; col. 4, ll. 54 to 56). After a data communication link is activated between the two devices, data for performing an authentication session is transferred between the devices B and M (Figure 2, steps 202 to 206; col. 8, ll. 60 to 64). The first authentication session at consumer device M generates a first key k1 (Figure 2, step 210; Abstract; col. 9, ll. 6 to 10). Thereafter, Herlin transmits data between the devices M and B to perform a subsequent authentication session (Figure 2, step 216; col. 9, ll. 10 to 12). A second authentication session at consumer device B generates a second key k2 (Figure 2, steps 218 to 222, and 226; col. 9, ll. 12 to 26). The Abstract in Herlin clearly explains that the second key k2 "is used in both the authentication process and as the key for encrypting subsequent communications" between the devices. Herlin transfers audio as well as visual content between the devices (col. 6, l. 64 to col. 7, l. 42).

In a second embodiment, Herlin generates three different keys k1, k2, and k3 during three different authentication sessions (Figures 4A and 4b, steps 402, 440, and 462, respectively; col. 10, l. 43 to col. 11, l. 63).

The Examiner relied on Jaisimha for a teaching of "a media player and media server that exchange audio or visual content, (Col 4 lines 36-42)" (Ans. 4).

The Examiner relied on the Bluetooth publication for a teaching of "using a first key and a second key and merging them in an XOR fashion to create a new link key, page 156 lines 1-3" (Ans. 5).

The Examiner relied on Holloway for a teaching of "encrypting one key with another and sending it to a recipient, (Col 9 lines 45-53)" (Ans. 5).

The Examiner relied on Crane for a teaching of "APIs with cryptographic operations and a common data security architecture, (Col 4 lines 19-25, 56-65)" (Ans. 6).

The Examiner relied on Moskowitz for a teaching of "limiting the quality of media based on authorization rights, (Col. 4 lines 35-50)" (Ans. 6).

PRINCIPLES OF LAW

The Examiner bears the initial burden of presenting a prima facie case of obviousness. *In re* Oetiker, 977 F.2d 1443, 1445 (Fed. Cir. 1992). If that burden is met, then the burden shifts to the Appellant to overcome the prima facie case with argument and/or evidence. *See Id.*

The Examiner's articulated reasoning in the rejection must possess a rational underpinning to support the legal conclusion of obviousness. *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006).

"The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR International Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1739 (2007).

During ex parte prosecution, claims must be interpreted as broadly as their terms reasonably allow since Applicants have the power during the administrative process to amend the claims to avoid the prior art. *In re Zletz*, 893 F.2d 319, 321-22 (Fed. Cir. 1989).

ANALYSIS

As indicated *supra* in the findings of fact, Herlin describes a Figure 2 embodiment that generates two different keys during two different authentication sessions as set forth in claims 1, 9, 12 to 15, 17, and 19 on appeal. In the Figure 4 alternative embodiment, Herlin generates three different keys during three different authentication sessions between more than two consumer devices. Nothing in claim 1 on appeal limits the broadly claimed "consumer devices" to just two consumer devices. The Abstract in Herlin teaches that the second key is used during transfer of audio as well as visual content between the devices (Br. 7 and 8). Thus, the teachings of Jaisimha are merely cumulative to the audio and visual content teachings already found in Herlin.

Turning to claim 3, the flowcharts in Figures 2 and 4 of Herlin show that the "authentication sessions are performed independent of each other."

With respect to claim 4, the "additional data" transmitted between the devices is performed in step 216 in Figure 2 of Herlin.

We agree with the Examiner's finding that "Herlin teaches means for receiving information and decrypting the information using a link key, (Col 5 lines 45-50)" (Ans. 4) (claim 11).

Turning next to claims 2, 5, and 16, we agree with the Examiner's finding that it would have been obvious to the skilled artisan "to combine the first and second keys of Herlin to create a more secure system" based upon the Bluetooth publication teachings of "using a first key and a second key and merging them in an XOR fashion to create a new link key" (Ans. 5).

It would have been obvious to the skilled artisan "to use k1 of Herlin as the key encrypting key of k2" based upon the key merge teachings of Holloway (Ans. 5 and 14) (claim 8).

Based upon the teachings of Crane, we agree with the Examiner that it would have been obvious to the skilled artisan to provide Herlin with an Application Programmers Interface (API) "for greater flexibility for the design of the system" while "managing the keys and authentication process" (Ans. 6 and 14) (claim 10).

Turning lastly to claims 18 and 20, we agree with the Examiner's finding that the skilled artisan would have found it obvious to limit the quality of media in Herlin based on authorization rights as taught by Moskowitz (Ans. 6).

CONCLUSION OF LAW

The Examiner has established the obviousness of claims 1 to 5 and 8 to 20.

ORDER

The obviousness rejection of claims 1 to 5 and 8 to 20 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

KIS

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P. O. BOX 3001
BRIARCLIFF MANOR, NY 10510